



***Cabinet for Health and Family Services (CHFS)  
Information Technology (IT) Policy***



***070.207 E-mail Distribution Lists***




**Version 2.3  
October 25, 2018**

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

## Revision History

Date	Version	Description	Author
9/1/2002	1.0	Effective Date	CHFS IT Policies Team Charter
10/25/2018	2.3	Review Date	CHFS OATS Policy Charter Team
10/25/2018	2.3	Revision Date	CHFS OATS Policy Charter Team

## Sign-Off

Sign-off Level	Date	Name	Signature
Executive Advisor (or designee)	10/25/2018		
CHFS Chief Information Security Officer (or designee)	10/25/2018	DENNIS E. LEBER	

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

## Table of Contents

<b>1</b>	<b>POLICY DEFINITIONS.....</b>	<b>4</b>
<b>2</b>	<b>POLICY OVERVIEW.....</b>	<b>6</b>
2.1	PURPOSE .....	6
2.2	SCOPE .....	6
2.3	MANAGEMENT COMMITMENT.....	6
2.4	COORDINATION AMONG ORGANIZATIONAL ENTITIES .....	6
2.5	COMPLIANCE .....	6
<b>3</b>	<b>ROLES AND RESPONSIBILITIES .....</b>	<b>6</b>
3.1	CHIEF INFORMATION SECURITY OFFICER (CISO) .....	6
3.2	CHIEF PRIVACY OFFICER (CPO) .....	7
3.3	SECURITY/PRIVACY LEAD .....	7
3.4	CHFS CONTRACT, STATE, AND VENDOR STAFF/PERSONNEL .....	7
3.5	SYSTEM DATA OWNER AND SYSTEM DATA ADMINISTRATORS.....	7
<b>4</b>	<b>POLICY REQUIREMENTS .....</b>	<b>8</b>
4.1	GENERAL .....	8
4.2	REQUESTING A NEW DISTRIBUTION LIST .....	8
<b>5</b>	<b>POLICY MAINTENANCE RESPONSIBILITY .....</b>	<b>9</b>
<b>6</b>	<b>POLICY EXCEPTIONS .....</b>	<b>9</b>
<b>7</b>	<b>POLICY REVIEW CYCLE.....</b>	<b>9</b>
<b>8</b>	<b>POLICY REFERENCES .....</b>	<b>9</b>

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

# 1 Policy Definitions

- **Cabinet Level:** The purpose of these lists is to send out information or alerts pertinent to staff from all organizations within the Cabinet. Use of these lists is restricted to the Office of the Secretary, the Office Human Resources Management (OHRM), and OATS.
- **Confidential Data:** COT standards define confidential data as the data the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modifications, breach, or destruction of that data. Examples include, but are not limited to, data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.
- **Contract Staff/Personnel:** An employee hired through a state approved (i.e. System Design/Development Services {SDS} Vendor Agreement/Company) vendor who has a master agreement with the state.
- **Departmental Level:** These distribution lists are used for communications directed at a single department or office within the Cabinet. A primary and alternate designated owner will be appointed by each Commissioner or Executive Director. This appointee will be responsible for ensuring the proper usage of the list and will periodically review the list for correctness.
- **Electronic Personal Health Information (ePHI):** Any protected health information (PHI) that is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in an electronic form.
- **Enterprise Identity Management (EIM):** Identity management solution used to provide internal users with network service entitlements.
- **Federal Tax Information (FTI):** Information received from the Internal Revenue Service (IRS) or secondary source, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service, that includes tax information. Examples would be an individual's tax return or anything that the IRS collects and that the IRS is going to use in order to determine a person's tax liability or potential tax liability.
- **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity (i.e. name, Social Security number, biometric records, etc.). PII can be the individual's personal information or is identified when combined with other personal or identifiable information (i.e. date of birth, birth place, mother's maiden name, etc.).
- **Sensitive Data:** Defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to, information identifiable to an individual (i.e. dates of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) and Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

- **State Staff/Personnel:** An employee hired directly through the state within the CHFS.
- **User Defined:** These lists may be used to correspond with a group of email users who may or may not be within a single Cabinet organizational unit. These groups are designed around a “business purpose” or “area of interest”. Examples include groups such as timekeepers, wireless coordinators, personnel liaisons, EEO Coordinators, etc. These lists must be owned by a Cabinet employee who is a member of the list. The owner will be responsible to oversee the appropriate use of the list and to periodically review the list for accuracy.
- **Vendor Staff/Personnel:** An employee contracted through an approved Master Business Associate Agreement, or other formal agreement, to provide temporary work for CHFS.

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

## 2 Policy Overview

### 2.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish a comprehensive level of security controls through an e-mail distribution policy. This document establishes the agency's E-mail Distribution Lists Policy to manage risks and provide guidelines for security best practices regarding lists created for information distribution through e-mail.

### 2.2 Scope

The scope of this policy applies to all internal CHFS state, contract, and vendor staff/personnel, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems.

### 2.3 Management Commitment

OATS Division Directors, the CHFS Chief Technical Officer (CTO), Chief Information Security Officer (CISO), and IT Executive Management have reviewed and approved this policy. Senior Management supports the objective put into place by this policy. Violations of not abiding by this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. CHFS shall report illegal activities or theft of CHFS property (physical or intellectual) to the appropriate authorities.

### 2.4 Coordination among Organizational Entities

OATS coordinates with CHFS organizations and/or agencies that access applications, systems, and facilities. All organizational entities that interact with CHFS are subject to follow requirements outlined within this policy.

### 2.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in applicable state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Additionally, applicable agencies follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

## 3 Roles and Responsibilities

### 3.1 Chief Information Security Officer (CISO)

Individual responsible for providing guidance and direction in assessment, planning, and implementation of all security standards, practices, and commitments required. This individual is responsible for adherence to this policy.

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

### **3.2 Chief Privacy Officer (CPO)**

An individual responsible for overseeing activities related to the development, implementation, maintenance of, and adherence to the Cabinet's and Commonwealth's information privacy and confidentiality policies and procedures in compliance with federal and state laws. This individual will conduct Health Insurance Portability and Accountability Act (HIPAA) risk analysis through coordination with the Information Security Agency Representative, the CISO, or CHFS OATS Information Security (IS) Team, and other CHFS agencies, and will ensure compliance with HIPAA notification and reporting requirements in the event of an identified breach.

### **3.3 Security/Privacy Lead**

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate staff/personnel. This individual(s) is responsible for providing privacy and security guidance and direction for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff/personnel. This role along with the CHFS OATS IS Team is responsible for adherence to this policy.

### **3.4 CHFS Contract, State, and Vendor Staff/Personnel**

All CHFS contract, state, and vendor staff/personnel must adhere to this policy. All staff/personnel must comply with referenced documents, found in section [8 Policy References](#) below that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

### **3.5 System Data Owner and System Data Administrators**

Management/lead who works with the application's development team, to document components that are not included in the base server build, and ensures that functionality and backups are conducted in accordance with business needs. This individual(s) is also responsible for working with personnel within the enterprise, agency, application, technical and business areas, for providing full recovery of all application functionality, as well as meeting federal and state regulations for disaster recovery situations.

<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

## 4 Policy Requirements

### 4.1 General

The Cabinet for Health and Family Services (CHFS) manages the use of Email Distribution lists as described in this policy. For the purposes of this policy, distribution lists are categorized into three groups:

- Cabinet
- Departmental
- User Defined

Distribution lists are established and owned by the Commonwealth Office of Technology (COT). These lists should be requested through [CHFSServiceRequests@ky.gov](mailto:CHFSServiceRequests@ky.gov) for a Distribution List to be created. Once the distribution lists are created, regardless of category, they must have a designated owner (a CHFS Employee) who will be responsible to oversee the appropriate use of the list and to periodically review the list for accuracy.

Attachments should be avoided, if possible. Users should utilize links to shared sites to provide access to documents. Brevity is always encouraged. The owner can designate additional employees to have pre-approval access to the list.

CHFS OATS IS Team recommends that a confidentiality statement be included on cabinet, departmental, and user defined distribution lists as well as individual email communications below the user's signature line. Example of a confidentiality statement would include, but is not limited to:

- This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and any disclosure, copying, or distribution of this message, or the taking of any action based on it, by you is strictly prohibited.

### 4.2 Requesting a New Distribution List

Requests for new distribution lists must be agreed upon with the agency's Branch Manager and ultimately approved by:

- Cabinet- Secretary's Office
- Departmental- Commissioner's or Executive Directors Office
- User owned lists- appropriate Branch Manager or Director whose employee will serve as the designated owner

Once approved, requests for establishing an email distribution list should be forwarded to [CHFSServiceRequests@ky.gov](mailto:CHFSServiceRequests@ky.gov) for processing.

Modifications the Active Directory (AD) user's accessibility to the list(s) can be updated by the designated owner of the distribution list.



<a href="#">070.207 E-mail Distribution Lists Policy</a>	Current Version: 2.3
070.000 Administrative	Review Date: 10/25/2018

## 5 Policy Maintenance Responsibility

The OATS IS Team is responsible for the maintenance of this policy.

## 6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

## 7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

## 8 Policy References

- [Centers for Medicare and Medicaid Services \(CMS\) MARS-E 2.0](#)
- [CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy](#)
- [Enterprise IT Policy: CIO-084- E-mail Review Request Policy](#)
- [Internal Revenue Services \(IRS\) Publication 1075](#)
- [Kentucky Revised Statute \(KRS\) Chapter 61.878 Certain public records exempted from inspection except on order of court – Restriction of state employees to inspect personnel files prohibited](#)
- [National institute of Standards and Technology \(NIST\) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations](#)
- [Social Security Administration \(SSA\) Security Information](#)